Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-20. (Cancelled)

21. (Currently Amended) A method for authenticating a user for access to at least two entities of a data transmission network by means of a terminal, which method includes the following series of steps:

- a random number is transmitted to the terminal,
- data for authenticating the user to the two entities of the network is calculated using at least one predefined cryptographic algorithm applied to the random number received and at least one secret key specific to the user,
- the terminal inserts, in an access request, data for identifying the user to said two entities of the network and the calculated authentication data, and transmits the access request to an access controller, wherein the inserted data for authenticating ~~identifying~~ the user comprises a distinct set of data for each of the two entities;
- the access controller transmits, to each of the two entities, a respective authentication request containing the identification data and the distinct set of inserted data for authenticating the user to the respective entity of the network, contained in the access request,
- authentication servers of the entities carry out a user authentication procedure, on the basis of user identification and authentication data, contained in the authentication requests, and
- authentication reports containing results of the authentication procedures carried out by the authentication servers of each of said two network entities are transmitted to the terminal.

22. (Previously presented) The method according to claim 21, characterized in that it includes a preliminary step in which the terminal establishes a connection with a specialized server by means of the network, wherein the random number is generated and transmitted to the terminal by the specialized server when the connection has been established.

23. (Previously presented) The method according to claim 22, characterized in that the access request transmitted by the terminal is transmitted to the specialized server which inserts therein the random number used to calculate the authentication data, the access request is then transmitted to the access controller which inserts the random number into the authentication requests transmitted to the two entities.

24. (Previously presented) The method according to claim 21, characterized in that the identification data inserted into the access request is in the form: "IdA@DomainA" in which:

- "IdA" represents the identifier for identifying the user to the network entity,
- "DomainA" represents the identifier of the network entity in the network, with the access controller determining the entities to whom the authentication requests will be transmitted on the basis of the "DomainA" identifiers of the network entity contained in the access request.

25. (Previously presented) A user terminal capable of accessing, by means of the access network, at least two entities connected to a data transmission network:

characterized in that it includes:

- means for transmitting access requests to at least two entities of the network, which requests contain data for identifying and authenticating the user to the network entity and each request being distinct;
- means for receiving a random number when a connection with the network is established, cryptographic calculating means for applying at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to at least two entities of the network, and means for inserting, into each transmitted access request, data for identifying the user to each network entity and the calculated authentication data,

wherein the calculated authentication data comprises a distinct set of authentication data for each entity .

26. (Previously presented) The terminal according to claim 25, characterized in that it includes an external module designed to be connected to each of the user terminals and including means for receiving the random number from the terminal to which it is connected, cryptographic calculation means for executing the predefined cryptographic algorithm based on the random number, and for transmitting, to the terminal, at least one data item for authenticating the user to an entity of the network, obtained by the cryptographic calculations.

27. (Previously presented) An access controller, characterized in that it includes means for receiving a request for access to at least two entities of a data transmission network coming from a user terminal and transmitted via said network, means for extracting, from the access request, the data for identifying and authenticating the user to at least two network entities, wherein the data for authenticating the user to at least two network entities comprises a distinct set of data for each of the network entities, means for transmitting, to each of the two entities, a respective authentication request containing the data for identifying and authenticating the user to a respective one of the two entities, contained in the access request.

28. (Previously presented) The access controller according to claim 27, characterized in that it also includes means for receiving user authentication reports, transmitted by the entities in response to the authentication requests, and means for transmitting, to the user terminal, and authentication report based on the reports received from the entities.

29. (Previously presented) A system for authenticating a user in an attempt to access at least two entities of a data transmission network to which network entities are connected, and which user terminals can access by means of access networks, characterized in that it includes:

- a user terminal characterized in that it includes:
- means for transmitting access requests to an entity of the network, which requests contain data for identifying and authenticating the user to the network entity; and

- means for receiving a random number when a connection with the network is established, cryptographic calculating means for applying at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to at least two entities of the network, and means for inserting, into each transmitted access request, data for identifying the user to two network entities and the calculated authentication data, wherein the calculated authentication data comprises a distinct set of data for each of the network entities;

- at least one authentication server for each of the two network entities, designed to identify and authenticate the users on the basis of identification and authentication data contained in the access requests received;

- an access controller characterized in that it includes means for receiving requests for access to at least two entities of the data transmission network coming from user terminals and transmitted via said network, means for extracting, from each of the access requests, the data for identifying and authenticating the user to at least two network entities, means for transmitting, to each of the two entities, a respective authentication request containing the data for identifying and authenticating the user to the two entities, contained in the access request.

30. (Previously presented) The system according to claim 29, characterized in that it also includes a specialized server connected to the network so as to be connected to the user terminals when a connection has been established between the terminal and the network, wherein the specialized server includes means for generating and transmitting a random number to each of the terminals with which a connection is established, and means for inserting the random number into each of the access requests transmitted by the terminals.

31. (Previously presented) The system according to claim 29, characterized in that each entity of the network includes means for storing secret keys of users, means for determining the data for authenticating the user to the entity by applying the predefined algorithm to the random number received in a authentication request and to the secret user key, and for comparing the result obtained to the user authentication data received in the authentication request, wherein the

user is properly authenticated by the entity only if the result of the cryptographic calculation obtained is identical to the authentication data contained in the authentication request.